FROM THE EDITOR | JOHN DIX

The water pump alarm

If nothing else, the now disputed "hacking" of an Illinois water utility has brought the spotlight back on the vulnerability of our national infrastructure.

This subject goes in and out of vogue in various government circles, yet we still seem to be treading water, waiting for a real attack to make us serious about addressing the threat.

Many thought the early reports out of Springfield on Nov. 10 were the opening salvo. That day, the Illinois Statewide Terrorism & Intelligence Center (STIC) issued a report titled "Public Water District Cyber Intrusion."

The report said someone in Russia had hacked into a SCADA contractor and purloined credentials that were then used to access controls in Springfield's Curran-Gardner Public Water District. By repeatedly cycling a pump on and off, it was believed the attacker managed to cause that device to fail. (See story, page 10.)

If true, the incident would be the first reported domestic attack on a utility from a foreign land to result in damage, and potentially portend more significant attacks.

The FBI and Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) have since concluded there was no evidence of an attack, but the way the whole incident unfolded is reason enough for concern.

Consider the glacial response. Illinois issued the report on a Thursday. ICS-CERT didn't become aware of it until the following Wednesday. If the incident was real — and there was no evidence at the time that it was anything but — shouldn't alarm bells have started to ring upstream somewhere? And while ICS-CERT did jump on some log analysis when it finally became aware of the event, it didn't actually send a team in to investigate until many days after that.

In the post 9/11 era, is this adequate? One would think not given that, one, the very existence of the ICS-CERT is acknowledgement enough that the threat is to be taken seriously. And two, DHS acknowledges there have already been intrusions. Greg Schaffer, acting deputy undersecretary of the Department of Homeland Security's National Protection and Programs Directorate, was quoted in the *Washington Post* saying the bad guys "are knocking on the doors of these systems. In some cases, there have been intrusions" (see the story at tinyurl.com/3nvctar).

While this whole incident increasingly appears to have been a false alarm, the real alarm is our lackadaisical response. Addressing the process for reacting to events is a lot easier than addressing the inadequacies of infrastructure security, yet evidently we haven't even gotten that right yet.

What's it going to take before the government mandates that national infrastructure security is brought in line with enterprise network security? Unfortunately, I think we all know the answer to that.

inside

DECEMBER 5, 2011